PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Project MESA Support
Wireless Security Recommendations
White Paper

FINAL

September 2002

INTRODUCTION

This document outlines the Public Safety Wireless Network (PSWN) Program's recommendations for wireless data security for Project MESA's Statement of Requirements (SoR) document. The first version of the SoR is scheduled for release subsequent to the fifth plenary meeting to be held in Copenhagen, Denmark, on September 25–27, 2002.

Project MESA is a cooperative global effort to establish technology standards for the development of the next generation of wireless data devices, systems, and applications. This standards development project is co-sponsored by the European Telecommunications Standards Institute (ESTI) and the Telecommunications Industry Association (TIA), and in conjunction with various public safety and protection, disaster relief, and peacekeeping entities and the vendor community.

Currently, Project MESA is continuing the first phase of a projected multiphased effort for the development of advanced mobile broadband data communications technology. This first phase is the development of the SoR that will incorporate a common global view of potential applications and services, from a user standpoint, that will require significant bandwidth for adequate operation and efficiency. The subsequent phase, which will be developed in response to the SoR, will elaborate, approve, and maintain the required set of technical specifications and reports that will culminate in the preliminary design of a mobile broadband system.

During the most recent planning session in Mesa, Arizona, in April 2002, Mr. Rick Murphy (Department of Treasury/PSWN) was appointed to chair an ad hoc committee to further discuss and define various security elements for incorporation in the latest version of the SoR. The program's understanding, as outlined, is the result of continuing research and investigation of a variety of wireless security initiatives that are currently available or are emerging technologies.

The Project MESA concept is far-reaching, and the transport media are still to be defined; therefore, the potential for Project MESA compliant networks, applications, and devices to use an array of different connective media remains a significant possibility. Based on that understanding, this paper provides—

- An overview of the wireless security environment discussing the continuing threats, emerging standards, and potential solutions

- A suggested deployment of a three-level system of wireless security that provides sufficient applications and information security based on low, medium, or high protection needs

- A proposed three-level security architecture using layers of different security technologies incorporating—
  - Next-generation crypto-engines
  - Security firmware
  - Applications programming interface (API)
  - Security applications and peripheral devices

- A conclusion presenting a summary of recommendations for discussion and potential inclusion within the final version of the SoR.

UNDERSTANDING THE ENVIRONMENT

The fragile security of wireless applications and wireless networks continues to be abundantly evident across the world with malicious attacks occurring on a daily basis. In Japan, virus-infected e-mails sent to wireless handsets, in some cases, generated repeated calls to Japan's national emergency number or caused several long distance calls to be made without the user's knowledge. In other instances, subscriber units "froze up," making it impossible for system users to access any of the carrier's services.

Incidents like this one and others involving "spamming," denial-of-service, virus attacks, content piracy, and malicious hacking are becoming commonplace occurrences in today's technology landscape. The proliferation of 802.11 standards based wireless local area networks (WLAN) with their well known and publicized security deficiencies only add to the difficulties facing potential public safety users. The security breaches that have posed a constant threat to desktop computers and enterprise networks over the last 10 years are migrating to the world of wireless communications where they will pose a threat to mobile telephones, smart telephones, personal digital assistants (PDA), laptop computers, and other yet-to-be-invented devices that capitalize on the convenience of wireless communications. Project MESA networks, applications, and devices will not be immune to these security threats.

Unfortunately, protecting wireless communications and the applications that use WLANs is proving significantly more difficult than securing desktop computer applications and enterprise networks. In contrast with wireless devices, desktop computers, and servers have limited and identifiable points of entry, and these entry points can be controlled and safeguarded. However, with wireless communications, important and often vital information is frequently placed on a mobile device that is vulnerable to theft and loss. In addition, this information is often transmitted over the unprotected airwaves in both wide-area commercial public and private wireless data systems and WLANs. Some emerging applications such as mobile-commerce (m-commerce) require that critical information be decrypted by a server somewhere in the communications chain before it is encrypted again and forwarded to its destination. Every point in the wireless communications chain where information is decrypted represents a potential vulnerability in the security of the system.

Addressing the question of wireless security is not simple because the wireless marketplace is far from monolithic. Deploying significant, yet unwarranted, security measures on applications or infrastructure components would only frustrate users by slowing down the responsiveness of the application or component. Not all transactions, applications, or information require the most strenuous security protection. Receiving incident data regarding a barking dog complaint from a computer-aided dispatching (CAD) system must be fast and spontaneous, but does not require significant degrees of high security. Security measures must match the nature of the application and the criticality of the information to ensure satisfied users and maintain efficiency. At the same time, the security should be strong enough to instill a sense of trust that the transaction does not jeopardize personal information, privacy, or place public safety personnel in a position of risk.

Ultimately, the users of Project MESA enabled wireless communications may be quite varied, ranging from law enforcement, fire protection personnel, emergency medical workers, disaster readiness and recovery agencies, and many non-traditional public safety and public protection groups with diverse expectations and requirements. As a result, the applications, types of wireless terminal devices, the connective networks, and usage patterns may vary widely. Commercial carriers may seek to provide differentiated service offerings for the variety of MESA services and users. Private networks or WLAN extensions of enterprise networks may also be used to provide the required connectivity to support MESA applications for the various public safety and public protection users. Simultaneously, mobile device original equipment manufacturers (OEM) may want to simplify and reduce development and deployment costs by settling on a basic terminal device architecture that is flexible, adaptable, scalable, and powerful enough to minimize or prevent security threats over an extended period of time and potentially over a variety of different networks.

Suppliers of the basic architecture components for the MESA wireless devices must have in-depth knowledge and real-world experience regarding the public safety and public protection environment. It is imperative to understand how critically important security will be to the success of Project MESA compliant applications, devices, and infrastructure components. The Project MESA device architecture must be sufficiently robust to enable it to support the most complex and demanding security protocols, applications, and algorithms, but it should be scalable and adaptable to the simplest of security applications. The architecture should maintain and support compatibility with a wide range of third-party security software and hardware, selected based on open standards or industry accepted "best practices." The proposed security platform should provide a total security solution for commercial carriers, private wireless networks, WLANS, OEMs, and users.

LEVELS OF SECURITY

For various reasons dictated by existing government statutes and regulations, the security measures associated with many public safety type transactions, national security information, medical records information, etc., would require strong levels of encryption and security. However, a "one-size-fits-all" security approach would burden low-level applications or information with unnecessary complexities, hampering their spontaneous use or transfer. In contrast, high-level transactions or downloads involving significant information of high security value will require the strongest security measures, even if it means that the execution of the transaction will take a little longer. A slight delay is a small price to pay for a secure transaction.

The benefits of a robust measured security platform for Project MESA end users should be reflected by—

- Encouraging a high-level of trust and data integrity to support a wide-range of mobile real-time public safety event and informational content transactions over commercial, private networks, the Internet and virtual private networks (VPN)

- Easing the integration with standard browser-based applications and with non-browser-based applications

- Providing high-performance transactions and strong encryption including on-device, disposable key generation to create a highly secure environment for network transactions, public safety and public protection applications, mobile office applications, and enterprise VPN access

- Facilitating very fast secure transactions for applications involving high data transmission rates found in large file transfers, content and media distribution (streaming media), and other high-end high-date rata applications

- Enhancing users' experience through transparency, ease of use, and a flexible, adaptable, and scalable security and encryption environment

- Extending battery life of handheld devices with computationally sophisticated equipment while providing a highly secure environment

- Facilitating automatic, semi-automatic, and non-intrusive updates of security keys and algorithms using over-the-air rekeying (OTAR)[1] of user devices and subscriber units

- Providing updated device personalities consistent with a user's preferences and security authorizations using over-the-air programming (OTAP).[2]

To shape the right security measures for individual MESA applications, Project MESA planners, application developers, and equipment manufacturers must balance the expectations of the user community with the security requirements of the applications and the information to be accessed through these systems. This approach will cause the applications or the information to potentially fall into one of several levels.

Low-Level Security Needs

When important or personal information is not jeopardized or when the value of a wireless information transaction is fairly low, the security of applications and information can be adequately safeguarded with low-level encryption techniques and private and public key infrastructure (PKI) technology. Examples of these low-level applications or information sources may include—

- Dispatch messages or transactions

- Status updates for deployed vehicles or personnel

- Messaging between dispatchers and field units, stations and field units, or among field units for routine public safety purposes

[1] OTAR—over-the-air rekeying technology, which enables automatic key distribution to field deployed devices from a centrally located key generation facility. For more general information regarding OTAR see the PSWN Program document, "*Security Issues and Analysis Report – Encryption Key Management.doc"* at www.pswn.gov.

[2] OTAP—over-the-air programming is an emerging technology that allows the reprogramming of a field deployed communication device to support a different or modified user personality, security scheme, or feature/functionality set.

- Notifications of false alarms, or conditions involving non-hostile fires
- Status updates of fire hydrant availability or water main breaks
- Status updates of road closures for construction, maintenance, or other utility work that would prevent access by emergency vehicles
- Routine incident or event information from CAD system or records management system (RMS)
- Publicly accessible Web site or database content
- Local, state, and national non-criminal history inquiries
- Local, state, and national crime information "Hot File" inquiries
- Non-classified e-mail or other correspondence.

Users and information resources at this level are involved in routine transactions that require efficient and expedited responses. In the case of state and national criminal justice system information inquiries, responsiveness of the systems and components is prescribed by operating regulations. Keeping the user's expectations in mind, low-level security measures still must maintain the integrity of the information transmitted and received over the wireless communications channel while ensuring the authenticity and non-repudiation of the transaction.

Mid-Level Security Needs

The processing demands placed on the mobile device will increase from those required for low-level applications because more complex encryption, coupled with the presence of public and/or private key algorithms, in conjunction with a secure boot loader,[3] digital rights management, filtering and anti-spamming software, may required for mid-level applications. Adding stronger security techniques could come at the expense of responsiveness and the speed of general operations of the client device unless sufficient processing hardware modules can be included in the mobile device's architecture to accelerate security functions.

This level of security is consistent with what would be found in the commercial world when dealing with personal information such as driver's license numbers and credit card accounts, personal financial transactions such as bank deposits and withdrawals, or the buying and selling of stocks. Downloading copyrighted materials also requires security protection at this level. Examples of mid-level public safety applications or information sources may include—

[3] Boot Loader – A component of a computing device that contains enough logic to obtain startup programs from a permanent storage device. Boot loaders are usually found on read only memory (ROM) chips of computing devices.

- Messages identifying public safety personnel or civilians killed or injured before, during, or as a consequence of, any incident or incident response

- Transactions involving fire or life safety code inspections, violations, or investigations

- Access to transportation databases, such as Material Safety Data Sheets, the North American Guide Book to hazardous materials response, or other files that, if corrupted or altered, could change the course of action that a public safety or public protection agency may take to mitigate a transportation accident

- Messaging regarding the status of fire protection systems in an occupied building.

- Notifications of planned blasting operations

- Tactical or hostage rescue operations

- High-risk warrant services activities or law enforcement surveillance activities.

High-Level Security Needs

Generally, applications with high-level security needs will start with very strong encryption and PKI algorithms, and be enhanced from there. A dedicated hardware/software security module consisting of hardware-based random number generators, hardware-protected memory where root keys can be stored, secure input/output (I/O) channels, and accelerator modules to improve processing performance will be deployed at this level. This could be accomplished by implementing a security module integrated into the device's processor or by using an add-on security card such as a subscriber identity module (SIM)/wireless identity module (WIM) or a smart card, or by implementing an integrated on-chip security module. This level of security can potentially be supplemented with other add-on functionality such as biometric sensors for voice, fingerprint, facial geometry, and iris/retinal scanners as options.

Examples of these high-level public safety applications or information sources may include—

- Medical care messaging, including patient records, and treatment orders or any information consistent with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations

- Hazardous materials database inquiries, including those to the National Sheriffs' Association Databases and any transactions with Chemical Transportation Emergency Center (CHEMTREC)

- Transactions with locations required to prepare emergency plans under Superfund Amendments and Reauthorization Act of 1986 (SARA) Title III, " Emergency Planning and Community Right to Know Act;" and those required to notify their Local Emergency Planning Committee (LEPC) of any releases or accidents involving hazardous materials

- Access to locations of interest databases, which local agencies may use to flag calls to VIP addresses, places where suspected criminal organizations are known to frequent or operate, or where large quantities of hazardous materials are stored

- Hazardous cargo transfer messaging, including descriptions of carrier vehicles, escort vehicles, types of cargo, and quantities of cargo, routes of travel, or date/time of travel

- Messaging involving arson, bombings, or explosives investigations

- Any information dealing with weapons of mass destruction, terrorism intelligence, and dignitary protection

- Any transactions or information dealing with national security information.

Commercial applications at this end of the security spectrum will include those that involve very large monetary transactions, VPN access and mobile office applications, and content protection for very valuable software, information, or copyrighted video/audio files.

SECURITY ARCHITECTURE

With computer and communication security, the one constant in this advancing technology is continual change. As technology advances, hackers, software pirates, and other network users with malicious intent will continue to ply their trades and hone their skills. New security threats in the future will trigger new security techniques and technologies. Wireless users, commercial carriers, governmental agencies, and manufacturers will continually need to deploy new techniques to protect their subscribers and users.

As a consequence, developers, service providers, manufacturers, and carriers are realizing that the hardware and software architecture of the subscriber devices they support must be very scalable so it can support some or all of the components that might make up a complete security solution.

Applications and information will likely not require every single security component, but rather a baseline architecture consisting of various layers of protection that is flexible enough to meet the needs of each level in the users environment. This construct will simplify the development and deployment of new user applications and their associated security requirements. Additionally, the architecture should be adaptable to respond to and overcome new threats as they emerge. At the core of this architecture is a powerful crypto engine surrounded by firmware and an application-programming interface (API) to speed the integration of various security applications and peripherals.

CRYPTO ENGINE

The crypto engine for next-generation security should be a combination of hardware and software that is capable of protecting a device's resources from incursion and is able to safeguard communications from unauthorized interception and subsequent illicit use. The crypto engine should guard against the fraudulent use of the device and the services it provides. To facilitate these tasks, the crypto engine must be computationally robust and equipped with certain hardware-based accelerators tuned to the operations of cryptographic security algorithms. For example, the crypto engine should incorporate a true hardware-based random number generator, which forms the foundation of the security of the device. The random bytes generated by the random number generator create the secret or private keys used for encryption and decryption. The hardware accelerator modules of the crypto engine will empower efficient execution of common cryptographic algorithms. Table 1 identifies different symmetric and asymmetric key function technologies, as well as hashing techniques for message validation.

Table 1
Encryption Algorithms

Type of Algorithm	Algorithm Name
Symmetric	DES, 3DES, RC2, ARC4, AES
Asymmetric	RSA, DSA, DH, NTRU, ECC
Hash	SHA1, MD2, MD5

Applications requiring high-level security will demand a secure execution environment to protect the wireless subscriber unit from unauthorized access or incursion. The crypto engine must support a secure mode of operation in which sensitive information, and specifically cryptographic keys, will be protected from access or tampering by untrusted software or other malicious means.

SECURITY FIRMWARE AND APPLICATION PROGRAMMING INTERFACE

An important feature of security architectures is the cryptographic API that operates as the software interface component. The API must be flexible, supporting a wide range of cryptographic functions and allowing the crypto engine to interface with the higher levels of the hardware or software resident on the device. This may include any of several operating systems (OS) currently in use on mobile devices, industry-standard security protocols (i.e., SSL, WTLS, IPSec) and interfaces such as Microsoft's CAPI (crypto API) or PKCS (Public Key Cryptography Standards), which perform bulk encryption, key exchanges, and hashing algorithms. It may also interact with any add-on security software applications, such as VPNs, local firewalls, or other hardware peripherals. A side benefit of the API design in this type of security architecture is once it is implemented, the underlying crypto hardware should be modifiable or expandable for higher performance without changing any higher-level software.

The firmware layer should include a secure boot loader. This ensures that an OS or other system-level software programs that have been maliciously altered because of a security breach cannot control the system's hardware. When the system is powered up or reset, the boot loader, which is permanently stored in non-volatile memory, initializes the system-level software and brings up the operating system. Unfortunately, software contained in electronically alterable storage like flash memory is a security risk. For example, viruses embedded in Internet downloads, message traffic, or e-mails might modify OS software in flash memory, corrupt the operation of the host device, and potentially propagate themselves to other mobile devices.

Embedded read-only memory (ROM) is much more secure because it can only be modified by changing the hardware in the device. The secure boot loader could be placed in the on-processor ROM. As the secure boot loader initializes the system, it would only provide control to operating or system-level software that has been verified as safe and secure. The secure boot loader could make use of several public, private, or symmetric key techniques to verify the integrity of the OS software.

SECURITY APPLICATIONS AND PERIPHERALS

The third layer of this security architecture includes the industry-standard security protocols that the wireless device will need to interoperate with other devices and servers. This layer will also be composed of security applications like anti-virus programs, firewalls, software filters, and other software modules, which will be dictated by the requirements of the Project MESA enabled or defined applications operating on the mobile device.

Add-on security hardware modules should also be accommodated in this layer of the security architecture. These could include biometric peripherals, such as fingerprint readers or voice scanners, as well as other types of hardware modules that might accomplish voice encryption and other functions. Some of these hardware modules could be packaged in add-on cards or SIM/WIM cards so that they can be easily integrated into a mobile communications device when needed.

Many third-party security applications like firewalls, filtering mechanisms, and security protocols are currently considered industry-accepted building blocks. In addition, many of these "best-of-breed" solutions or components have demonstrated extensive interoperability with other security measures that are currently deployed in the marketplace. Project MESA's security requirements should leverage enhanced performance and security features inherent in these commercial offerings because of their longstanding acceptance in the marketplace and because they bring considerable value to the security makeup of wireless systems.

The proposed security architecture should incorporate extensive modularity for a variety of security algorithms, applications, and peripherals. The platform should function as a common programming environment for a wide range of hardware configurations, each matched to the processing requirements dictated by the user applications and security measures running on a particular mobile device.

CONCLUSION AND RECOMMENDATIONS

Security experts preach that hackers, software vandals, content pirates, and other security threats will never be eliminated. The tools of the hackers' trade—viruses, worms, and other assorted collections of malicious code—continue to morph and mutate into new and ever-increasing threats. As a result, hacking and other security threats cannot be fully defeated because they cannot be eliminated. However, individual security threats can be minimized by innovative and powerful security countermeasures. The foundation of any wireless security strategy must include sufficient processing power because the latency effects caused by wireless security measures will leave users frustrated and searching for alternative solutions. Conversely, handheld devices operating on battery power must incorporate designs to consume as little power as possible even when using the highest levels of encryption and security protection.

In light of these continuing threats and the stringent requirements of public safety and public protection entities for secure wireless data systems, the PSWN Program recommends consideration of the following—

- Recognition that Project MESA networks, applications, and devices will not be immune to security threats and that protecting wireless communications, applications, and information is proving significantly more difficult than securing desktop computer applications and enterprise networks.

- Understanding that not all transactions, applications, or information require the most strenuous security protection and the deployment of significant, yet unwarranted, security measures will only frustrate users and create inefficiencies.

- The critical importance of security and information integrity to the success of Project MESA compliant applications, devices, and infrastructure components.

- A security architecture that is sufficiently robust, scalable, and adaptable to support the most complex and demanding security protocols, applications, and algorithms.

- An architecture that maintains and supports compatibility with a wide range of third-party add-on security software (e.g. VPNs, firewalls, anti-virus programs, software filters) and hardware based upon open standards and/or industry-accepted "best practices."

- An architecture that supports different symmetric, asymmetric, and hashing technologies including DES, 3DES, RC2, ARC4, AES, RSA, DSA, DH, NTRU, ECC, SHA1, MD2, MD5.

- An architecture that supports multiple operating systems and industry-standard security protocols (e.g. SSL, WTLS, IPSec) and provides interfaces to Microsoft's CAPI and/or PKCS.

- A security platform that incorporates modularity for various security algorithms, applications, and peripherals that provides a total security solution for commercial carriers, private wireless networks, WLANs, OEMs, and users who will use or support Project MESA.

- The development of a robust, but measured security platform for Project MESA devices and networks and incorporation of low, medium, and high levels of security protections for information or applications at each level. The security levels from lowest to highest should incorporate more stringent requirements and capabilities based upon deployments of additional hardware, firmware, and software resources.

- A security platform that supports a wide range of hardware configurations that are matched to the processing requirements of user applications and security measures of the mobile device.

- A security architecture that incorporates a robust crypto engine, which will guard against the fraudulent use of the device and services. The engine should be a combination of hardware and software and support an embedded random number generator and hardware-based acceleration for optimization of cryptographic security algorithms.

- A proposed security architecture that supports add-on security hardware modules including biometric peripherals for fingerprint, voice, facial geometry, and iris/retinal scanning. The hardware should also incorporate support for SIM/WIM modules.

- Security requirements for Project MESA that leverage and expand on the enhanced performance and features inherent in commercial wireless security offerings.

To provide a secure mobile wireless data communications environment, one must identify the vulnerabilities, adopt a security strategy that takes into account all possible weaknesses, and deploy an architecture that is powerful enough to defeat today's threats, yet adaptable enough to meet the unimagined threats of tomorrow.